Configurazione di IP sovrapposti per la stessa VPN su più siti con scenari di errore

Sommario

Introduzione

Questo documento descrive lo scenario con spazi di indirizzi sovrapposti nella stessa VPN su più siti nella sovrapposizione SD-WAN. Illustra la rete di esempio, il comportamento del traffico in scenari normali/di failover, la configurazione e la verifica.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di SD-WAN.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- SD-WAN Controller versione 20.6.3
- Cisco IOS® XE (esecuzione in modalità controller) 17.6.3a
- Dispositivi host (CSR1000V) 17.3.3

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Qui potete trovare l'elenco degli acronimi utilizzati in questo articolo.

- Secure Internet Gateway - SIG
- Routing e inoltro virtuale - VRF
- Virtual Private Network - VPN
- Accesso diretto a Internet - DIA
- Network Address Translation - NAT
- Multi-Protocol Label Switching - MPLS
- Service Side Network Address Translation - SS-NAT
- Centro dati - DC
- Overlay Management Protocol - OMP
- Protocollo Internet - IP

Fare riferimento al documento Cisco per ulteriori dettagli sul lato servizio NAT: Service-side NAT

Esempio di rete

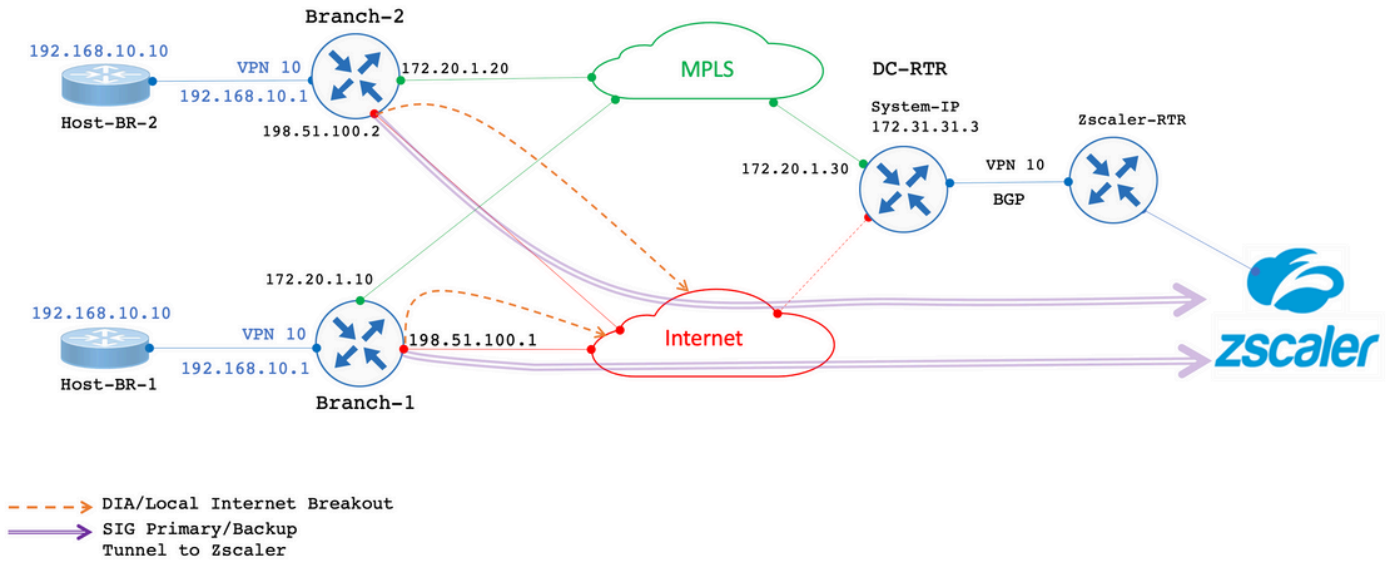
Nota: in questa topologia, i dispositivi ospitati nella VPN del servizio 10 di ciascun router di succursale hanno configurato IP 192.168.10.0/24 sovrapposto.

In questa topologia specifica, c'è 1 DC (il DC ha solo trasporto MPLS, ma in uno scenario reale possono esserci più trasporti) e 2 filiali con connettività a SD-WAN sovrapposta su MPLS e trasporto Internet. Service VPN 10 è configurato in tutte le posizioni. Per le filiali il tunnel SIG (primario e di backup) è configurato su Zscaler. DIA è configurato per alcuni IP di destinazione specifici in modo da ignorare lo Zscaler. In caso di errore del collegamento Internet alle succursali,

è previsto che tutto il traffico venga inviato al controller di dominio tramite il trasporto MPLS.

eBGP è configurato sul servizio VPN 10 con il router Zscaler all'estremità DC. Il router DC riceve il percorso predefinito dal router Zscaler e viene ridistribuito in OMP.

Nota: gli indirizzi IP pubblici menzionati in questo scenario di laboratorio sono tratti dalla documentazione RFC5737.



Specifiche

- Utilizzo di indirizzi IP sovrapposti per la filiale 1 e la filiale 2 sul lato servizio della VPN 10.

- In uno scenario tipico, quando MPLS e il trasporto Internet sono attivi, il traffico proveniente dalla VPN 10 deve uscire tramite tunnel SIG.
- Per i prefissi di destinazione IP specifici, il traffico deve ignorare il tunnel SIG e uscire tramite DIA.
- In caso di errore del collegamento Internet, tutto il traffico associato a Internet proveniente dalla VPN 10 deve essere chiuso tramite DC.

Soluzione

Per soddisfare tale requisito, SD-WAN dispone di Service Side NAT e DIA with Data policy.

- Il NAT del lato servizio è configurato su ciascun router di succursale con indirizzi IP diversi del pool NAT.
- In caso di errore del collegamento Internet quando il traffico viene inviato a SD-WAN overlay, l'IP di origine viene NAT all'indirizzo IP dal pool NAT configurato.
- Il router DC vede l'indirizzo post-NAT per le subnet sovrapposte.

Nota: per rappresentare il traffico normale attraverso il tunnel SIG dalla VPN 10, viene usato il protocollo IP 192.0.2.100 pubblico e, per una destinazione specifica, la porta DIA 192.0.2.1. Le configurazioni corrispondenti sono mostrate nella sezione di configurazione.

Configurazione

Configurazione Branch-1

La configurazione del router della filiale 1 è la seguente.

```
vrf definition 10
 rd 1:10
!
address-family ipv4
  route-target export 1:10
  route-target import 1:10
exit-address-family
!
interface GigabitEthernet2
description "Internet TLOC"
ip address 198.51.100.1 255.255.255.0
ip nat outside
!
interface GigabitEthernet3
description "MPLS TLOC"
ip address 172.20.1.10 255.255.255.0
!
interface GigabitEthernet4
description "Service Side VPN 10"
vrf forwarding 10
ip address 192.168.10.1 255.255.255.0
!
interface Tunnel2
ip unnumbered GigabitEthernet2
tunnel source GigabitEthernet2
tunnel mode sdwan
!
interface Tunnel3
ip unnumbered GigabitEthernet3
tunnel source GigabitEthernet3
tunnel mode sdwan
!
interface Tunnel100512
ip address 10.10.1.1 255.255.255.252
tunnel source GigabitEthernet2
tunnel destination 203.0.113.1
tunnel vrf multiplexing
!
interface Tunnel100513
ip address 10.10.1.5 255.255.255.252
tunnel source GigabitEthernet2
tunnel destination 203.0.113.2
tunnel vrf multiplexing
!
ip sdwan route vrf 10 0.0.0.0/0 tunnel active Tunnel100512 backup Tunnel100513
```

```
ip nat pool natpool1 172.16.2.1 172.16.2.2 prefix-length 30
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet2 overload
ip nat inside source list global-list pool natpool1 vrf 10 match-in-vrf overload
ip nat route vrf 10 192.0.2.1 255.255.255.255 global
!
ip route 0.0.0.0 0.0.0.0 198.51.100.100
ip route 0.0.0.0 0.0.0.0 172.20.1.100
!
```

Configurazione Branch-2

La configurazione del router Branch-2 è la seguente.

```
vrf definition 10
rd 1:10
!
address-family ipv4
route-target export 1:10
route-target import 1:10
exit-address-family
!
address-family ipv6
exit-address-family
!
interface GigabitEthernet2
description "Internet TLOC"
ip address 198.51.100.2 255.255.255.0
ip nat outside
!
!
interface GigabitEthernet3
description "MPLS TLOC"
ip address 172.20.1.20 255.255.255.0
!
interface GigabitEthernet4
description "Service Side VPN 10"
vrf forwarding 10
ip address 192.168.10.1 255.255.255.0
!
interface Tunnel2
ip unnumbered GigabitEthernet2
tunnel source GigabitEthernet2
tunnel mode sdwan
!
interface Tunnel3
ip unnumbered GigabitEthernet3
tunnel source GigabitEthernet3
tunnel mode sdwan
!
interface Tunnel100512
ip address 10.10.2.1 255.255.255.252
tunnel source GigabitEthernet2
tunnel destination 203.0.113.1
tunnel vrf multiplexing
!
interface Tunnel100513
ip address 10.10.2.5 255.255.255.252
```

```
tunnel source GigabitEthernet2
tunnel destination 203.0.113.2
tunnel vrf multiplexing
!
!
ip sdwan route vrf 10 0.0.0.0/0 tunnel active Tunnel100512 backup Tunnel100513
ip nat route vrf 10 192.0.2.1 255.255.255.255 global
ip nat pool natpool1 172.16.2.9 172.16.2.10 prefix-length 30
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet2 overload
ip nat inside source list global-list pool natpool1 vrf 10 match-in-vrf overload
!
ip route 0.0.0.0 0.0.0.0 198.51.100.100
ip route 0.0.0.0 0.0.0.0 172.20.1.100
!
```

Configurazione router DC

La configurazione del router DC è la seguente.

```
vrf definition 10
rd 1:10
!
address-family ipv4
route-target export 10:10
route-target import 10:10
exit-address-family
!
interface Tunnel2
ip unnumbered GigabitEthernet2
tunnel source GigabitEthernet2
tunnel mode sdwan
!
interface GigabitEthernet2
ip address 172.20.1.30 255.255.255.0
description "MPLS TLOC"
!
interface GigabitEthernet4
description "Service Side VPN 10"
vrf forwarding 10
ip address 172.31.19.19 255.255.255.252
!
router bgp 10
bgp log-neighbor-changes
distance bgp 20 200 20
!
address-family ipv4 vrf 10
redistribute omp
neighbor 172.31.19.20 remote-as 100
neighbor 172.31.19.20 activate
neighbor 172.31.19.20 send-community both
exit-address-family
!
!
ip route 0.0.0.0 0.0.0.0 172.20.1.100
!
```

Criterio vSmart

La configurazione dei criteri vSmart è la seguente.

Nota: **nat pool 1** viene chiamato nei criteri per entrambe le filiali, tuttavia, ci sono due diversi pool IP configurati per ciascuna filiale (172.16.2.0/30 per la filiale 1 e 172.16.2.8/30 per la filiale 2).

<#root>

data-policy _VPN10-VPN20_1-Branch-A-B-Central-NAT-DIA
vpn-list VPN10
sequence 1
match
source-ip 192.168.10.0/24
!
action accept

nat pool 1

```
!
default-action accept
!
site-list BranchA-B
site-id 11
site-id 22
!
site-list DC
site-id 33
!
vpn-list VPN10
vpn 10
!
prefix-list _AnyIpv4PrefixList
ip-prefix
```

0.0.0.0/0

```
 le 32
!
apply-policy
site-list BranchA-B
data-policy _VPN10_1-Branch-A-B-Central-NAT-DIA from-service
!
```

Scenari di failover

Scenario normale flusso traffico diramazione-1

Quando entrambi i trasporti sono attivi, come mostrato nell'output, per impostazione predefinita il traffico esce dal tunnel SIG **Tunnel100512**primario. Quando il tunnel primario diventa inattivo, gli switch passano al tunnel di backup **Tunnel100513**.

<#root>

Branch-1#

show ip route vrf 10

```
Routing Table: 10
<SNIP>
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S* 0.0.0.0/0 [2/0], Tunnel100512

 192.0.2.0/32 is subnetted, 1 subnets
n Nd 192.0.2.1 [6/0], 3d02h, Null0
n Ni 172.16.2.0 [7/0], 3d04h, Null0
m 172.16.2.8 [251/0] via 172.31.31.2, 3d01h, Sdwan-system-intf
Branch-1#
```

Il comando traceroute mostra che il traffico prende il tunnel SIG.

<#root>

Host-BR-1#

ping 192.0.2.100

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/49/101 ms
Host-BR-1#
```

Host-BR-1#

traceroute 192.0.2.100 numeric

```
Type escape sequence to abort.
Tracing the route to 192.0.2.100
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.10.1 38 msec 7 msec 4 msec
```

2 203.0.113.1

```
79 msec * 62 msec
Host-BR-1#
```

Il traffico diretto a una destinazione specifica **192.0.2.1** esce attraverso DIA (NATed to WAN IP address).

<#root>

Host-BR-1#

ping 192.0.2.1

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/49/101 ms
Host-BR-1#

Branch-1#sh ip nat translation
Pro Inside global Inside local Outside local Outside global
icmp
```

198.51.100.1:1

```
 192.168.10.10:1 192.0.2.1:1 192.0.2.1:1
Total number of translations: 1
Branch-1#
```

Scenario normale flusso traffico diramazione-2

Un comportamento simile viene osservato anche sul router Branch-2.

<#root>

Branch-2#

show ip route vrf 10

```
Routing Table: 10
<SNIP>
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
```

S* 0.0.0.0/0 [2/0], Tunnel100512

```
 192.0.2.0/32 is subnetted, 1 subnets
n Nd 192.0.2.1 [6/0], 00:00:08, Null0
m 172.16.2.0 [251/0] via 172.31.31.1, 3d01h, Sdwan-system-intf
n Ni 172.16.2.8 [7/0], 3d04h, Null0

Branch-2#
```

<#root>

Host-BR-2#

ping 192.0.2.100

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/49/101 ms
Host-BR-2#
```

```
Host-BR-2#t
raceroute 192.0.2.100 numeric


Type escape sequence to abort.
Tracing the route to 192.0.2.100
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.10.1 38 msec 7 msec 4 msec
2 203.0.113.1
79 msec * 62 msec
Host-BR-2#
```

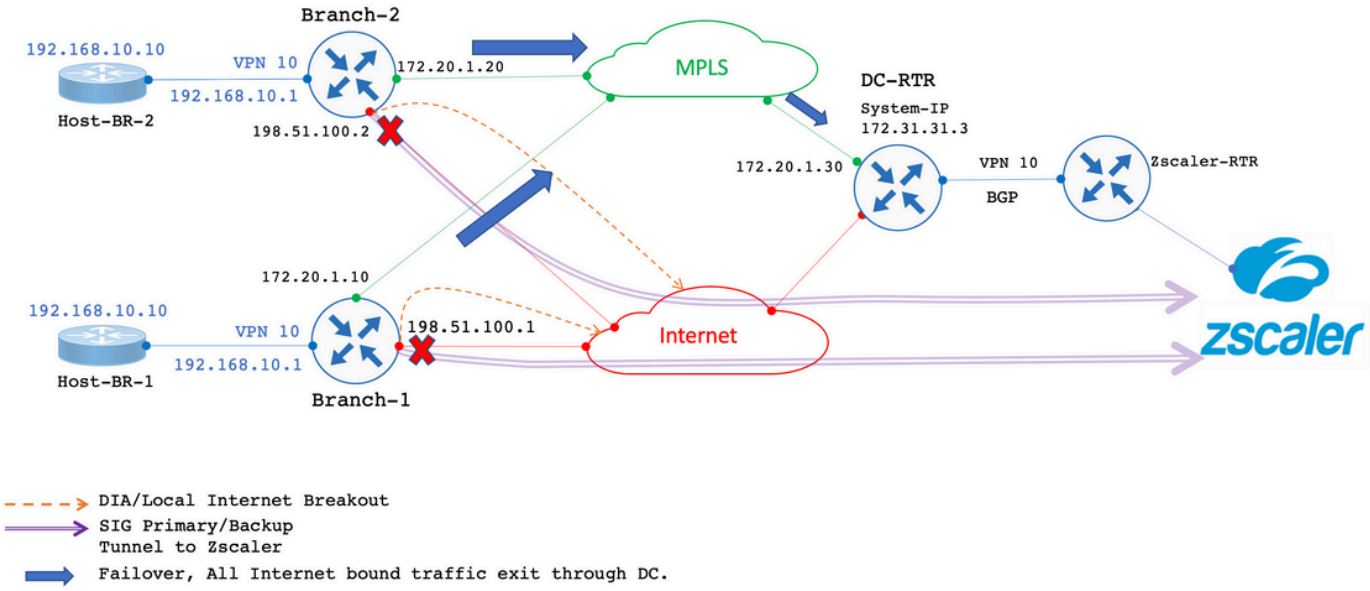
<#root>

```
Host-BR-2#
ping 192.0.2.1


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/49/101 ms
Host-BR-2#

Branch-2#
show ip nat translation


Pro Inside global Inside local Outside local Outside global
icmp
198.51.100.2:1
 192.168.10.10:1 192.0.2.1:1 192.0.2.1:1
Total number of translations: 1
Branch-2#
```

Scenari di errore

Scenario di errore di Branch-1

In questa sezione viene descritto il comportamento durante l'errore di Internet.



Il collegamento Internet viene chiuso a livello amministrativo per simulare un guasto a un collegamento Internet.

<#root>

Branch-1#

show sdwan control local-properties

```
<SNIP>
 PUBLIC PUBLIC PRIVATE PRIVATE PRIVATE MAX
INTERFACE IPv4 PORT IPv4 IPv6 PORT VS/VM COLOR STATE CNTRL

------------------------------------------------------------------------------------------------------------------------

GigabitEthernet2 198.51.100.1 12346 198.51.100.1 :: 12346 1/0 biz-internet down

GigabitEthernet3 172.20.1.10 12346 172.20.1.10 :: 12346 1/1 mpls up

Branch-1#
```

Gli output mostrano che durante lo scenario di errore del collegamento Internet, il router Branch-1 riceve il percorso predefinito dal router DC tramite OMP. **172.31.31.3** è l'IP del sistema per il router DC.

<#root>

Branch-1#

show ip route vrf 10

```
<SNIP>
Gateway of last resort is
```

172.31.31.3

 to network 0.0.0.0

m* 0.0.0.0/0 [251/0] via 172.31.31.3

, 00:01:17, Sdwan-system-intf
<SNIP>

Il traffico destinato a 192.0.2.100 il NAT viene reindirizzato al pool NAT del lato servizio e consente l'uscita tramite DC.

<#root>

Host-BR-1#

ping 192.0.2.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/37/103 ms
Host-BR-1#

<#root>

Branch-1#

show ip nat translations

Pro Inside global Inside local Outside local Outside global
icmp

172.16.2.1:3

 192.168.10.1:3 192.0.2.100:3 192.0.2.100:3
Total number of translations: 1
Branch-1#

I risultati del tracciamento routing mostrano che il traffico assume il percorso del controller di dominio. 172.20.1.30 è l'indirizzo IP della WAN di trasporto MPLS del router DC.

<#root>

Host-BR-1#

traceroute 192.0.2.100 numeric

Type escape sequence to abort.
Tracing the route to 192.0.2.100

```
  1 192.168.10.1 26 msec 5 msec 3 msec
```

```
  2 172.20.1.30
```

```
10 msec 5 msec 27 msec
<SNIP>
```

<#root>

Branch-1#

```
show sdwan bfd sessions
```

```
 SOURCE TLOC REMOTE TLOC DST PUBLIC DST PUBLIC DETECT TX
SYSTEM IP SITE ID STATE COLOR COLOR SOURCE IP IP PORT ENCAP MULTIPLIER INTERVAL(msec) UPTIME TRANSITION
--------------------------------------------------------------------------------------------------------
172.31.31.2 22 up mpls mpls 172.20.1.10 172.20.1.20 12406 ipsec 7 1000 0:14:56:54 0
```

```
172.31.31.3 33 up mpls mpls 172.20.1.10 172.20.1.30 12406 ipsec 7 1000 0:14:56:57 0
```

```
Branch-1#
```

Il traffico destinato a IP 192.0.2.1 specifico ottiene anche il NAT sul pool NAT del lato servizio ed esce tramite DC.

<#root>

Host-BR-1#

```
ping 192.0.2.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/37/103 ms
Host-BR-1#
```

<#root>

Branch-1#

```
show ip nat translations
```

```
Pro Inside global Inside local Outside local Outside global
icmp
```

```
172.16.2.1:4
```

```
 192.168.10.10:4 192.0.2.1:4 192.0.2.1:4
Total number of translations: 1
Branch-1#
```

<#root>

Host-BR-1#

traceroute 192.0.2.1 numeric

```
Type escape sequence to abort.
Tracing the route to 192.0.2.1

1 192.168.10.1 26 msec 5 msec 3 msec
```

2 172.20.1.30

```
10 msec 5 msec 27 msec
<SNIP>
```

Push della configurazione dei criteri dati da vSmart:

<#root>

Branch-1#

show sdwan policy from-vsmart

```
from-vsmart data-policy _VPN10-VPN20_1-Branch-A-B-Central-NAT-DIA
 direction
```

from-service

```
 vpn-list
```

VPN10

```
  sequence 1
   match
    source-ip
```

192.168.10.0/24

```
   action accept
    count NAT_VRF10_BRANCH_A_B_-968382210

nat pool 1

!
from-vsmart lists vpn-list VPN10
 vpn 10
!
Branch-1#
Branch-1#
```

show run | sec "natpool1"

```
<SNIP>
```

ip nat pool

natpool1

172.16.2.1

172.16.2.2

prefix-length 30

Scenario di errore Branch-2

Un comportamento simile viene osservato anche nei router della diramazione 2 quando è presente un failover di Internet.

<#root>

Branch-2#

show sdwan control local-properties

<SNIP>

PUBLIC PUBLIC PRIVATE PRIVATE PRIVATE MAX
INTERFACE IPv4 PORT IPv4 IPv6 PORT VS/VM COLOR STATE CNTRL

GigabitEthernet2 198.51.100.2 12346 198.51.100.2 :: 12346 1/0 biz-internet down

GigabitEthernet3 172.20.1.20 12346 172.20.1.20 :: 12346 1/1 mpls up

Branch-2#

<#root>

Branch-2#

show ip route vrf 10

<SNIP>
Gateway of last resort is

172.31.31.3

to network 0.0.0.0

m* 0.0.0.0/0 [251/0] via 172.31.31.3

, 00:10:17, Sdwan-system-intf
<SNIP>

<#root>

Host-BR-2#

ping 192.0.2.100

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/37/103 ms
Host-BR-2#
```

<#root>

Branch-2#

show ip nat translations

```
Pro  Inside global         Inside local          Outside local         Outside global
icmp
```

172.16.2.9:3

```
         192.168.10.1:3         192.0.2.100:3             192.0.2.100:3
Total number of translations: 1
Branch-2#
```

<#root>

Host-BR-2#

traceroute 192.0.2.100 numeric

```
Type escape sequence to abort.
Tracing the route to 192.0.2.100
  1 192.168.10.1 26 msec 5 msec 3 msec
```

2 172.20.1.30

```
10 msec 5 msec 27 msec
<SNIP>
```

<#root>

Host-BR-2#

ping 192.0.2.1

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.1, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/37/103 ms
Host-BR-2#
```

<#root>

Branch-2#

show ip nat translations

```
Pro  Inside global         Inside local          Outside local         Outside global
icmp
```

172.16.2.9:4

```
        192.168.10.10:4         192.0.2.1:4             192.0.2.1:4
Total number of translations: 1

Branch-2#
```

<#root>

Host-BR-2#

traceroute 192.0.2.1 numeric

```
Type escape sequence to abort.
Tracing the route to 192.0.2.1
  1 192.168.10.1 26 msec 5 msec 3 msec
```

2 172.20.1.30

```
10 msec 5 msec 27 msec
<SNIP>
```

<#root>

Branch-2#

show sdwan policy from-vsmart

```
from-vsmart data-policy _VPN10-VPN20_1-Branch-A-B-Central-NAT-DIA
 direction
```

from-service

```
 vpn-list
```

VPN10

```
  sequence 1
   match
    source-ip
```

192.168.10.0/24

```
   action accept
    count NAT_VRF10_BRANCH_A_B_-968382210
```

nat pool 1

```
!
from-vsmart lists vpn-list VPN10-VPN20
 vpn 10
!
Branch-2#
```

Branch-2#

show run | sec "natpool1"

```
<SNIP>
ip nat pool
```

natpool1

172.16.2.9

172.16.2.9

prefix-length 30

Stato routing router DC

La tabella di routing viene acquisita dal router DC.

Come mostrato nell'output, il router DC è in grado di distinguere gli indirizzi IP sovrapposti da entrambe le diramazioni con gli indirizzi **post-NAT IP**derivati dall'indirizzo **SS-NAT pool** (172.16.2.0 e 172.16.2.8) anziché dall'indirizzo IP della LAN effettiva **192.168.10.0/24172.31.31.1** e **172.31.31.2** sono gli indirizzi **system-ip** configurati per la diramazione 1/2. System-IP **172.31.31.10** appartiene a **vSmart**.

<#root>

DC-RTR#

show ip route vrf 10

```
Routing Table: 10
<SNIP>
m
```

172.16.2.0

```
 [251/0] via 172.31.31.1, 02:44:25, Sdwan-system-intf
m
```

172.16.2.8

```
 [251/0] via 172.31.31.2, 02:43:33, Sdwan-system-intf
m

192.168.10.0

[251/0] via

172.31.31.2

, 03:01:35, Sdwan-system-intf
 [251/0] via

172.31.31.1

, 03:01:35, Sdwan-system-intf


DC-RTR#

show sdwan omp routes


<SNIP> PATH ATTRIBUTE
VPN PREFIX FROM PEER ID LABEL STATUS TYPE TLOC IP COLOR ENCAP PREFERENCE
------------------------------------------------------------------------------------------------------------

10 172.16.2.0/30

 172.31.31.10 6 1002 C,I,R installed

172.31.31.1 mpls

 ipsec -
 172.31.31.10 10 1002 Inv,U installed 172.31.31.1 biz-internet ipsec -

10 172.16.2.8/30

 172.31.31.10 8 1002 C,I,R installed

172.31.31.2 mpls

 ipsec -

10 192.168.10.0/24

 172.31.31.10 1 1002 C,I,R installed

172.31.31.1 mpls

 ipsec -
 172.31.31.10 2 1002 C,I,R installed

172.31.31.2 mpls

 ipsec -
 172.31.31.10 12 1002 Inv,U installed

172.31.31.1

 biz-internet ipsec -
```

Verifica

Attualmente non è disponibile una procedura di verifica specifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Ulteriori informazioni

Scenario-1

Negli scenari in cui i controller si trovano nella versione 20.3.4 e cEdge esegue la versione 17.3.3a o versioni precedenti con le stesse configurazioni, si osserva che negli scenari normali/di failover il traffico raggiunge il pool NAT del lato servizio e interrompe il flusso.

cEdge acquisisce:

<#root>

Host-BR-1#

ping 192.0.2.100

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.100, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
Host-BR-1#
```

<#root>

Branch-1#

show ip nat translations

```
Pro Inside global Inside local Outside local Outside global
icmp
```

172.16.2.1

```
:3 192.168.10.1:3 192.0.2.100:3 192.0.2.100:3
Total number of translations: 1
Branch-1#

WOW-Branch-1#show run | sec "natpool1"
<SNIP>
ip nat pool
```

natpool1

172.16.2.1

172.16.2.2

prefix-length 30

L'output viene acquisito da cEdge eseguito sulla versione 17.3.3a. Il traffico destinato tramite il tunnel SIG raggiunge il pool NAT SS-NAT e viene scartato. Una correzione è disponibile a partire dalla versione 17.3.6.

Scenario-2

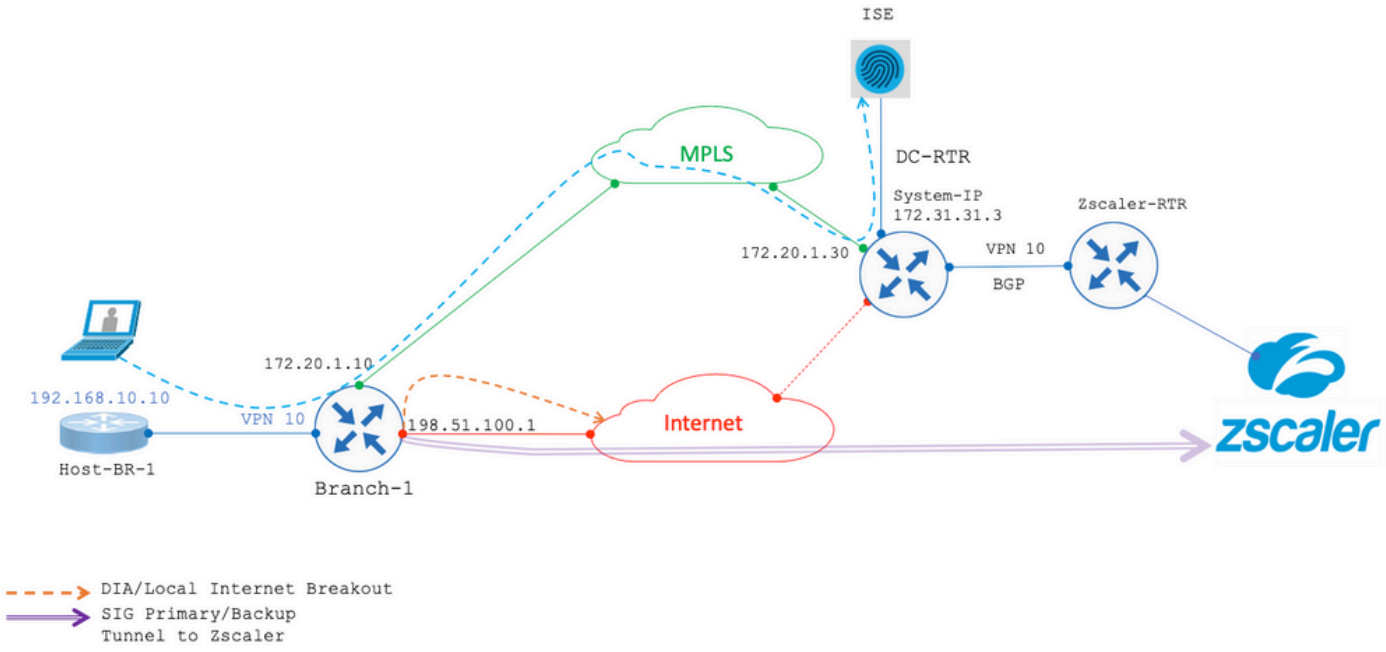
Requisito [Service Side NAT (SS-NAT) con ispezione UTD]

Si supponga che l'utente abbia richiesto i seguenti requisiti:

1. Quando sia Internet che i trasporti MPLS sono operativi, i client wireless della VPN 10 possono essere indirizzati all'ISE nel data center per l'autenticazione. Inoltre, il traffico VPN 10 che viaggia attraverso la sovrapposizione SD-WAN può essere sottoposto a ispezione. Poiché questo traffico fa parte della sovrimpressione, VPN 10 utilizza la funzionalità SS-NAT. [UTD + SS-NAT]

2. Se il trasporto via Internet non è più disponibile, tutto il traffico proveniente dalla VPN 10, incluso il traffico sia wireless che cablato, può essere indirizzato tramite la sovrimpressione utilizzando il trasporto MPLS. Anche questo traffico può essere soggetto a ispezione. [UTD + SS-NAT]

Questi requisiti mirano a garantire la sicurezza e il monitoraggio del flusso del traffico per VPN 10 nella filiale 1 in diverse condizioni di rete.



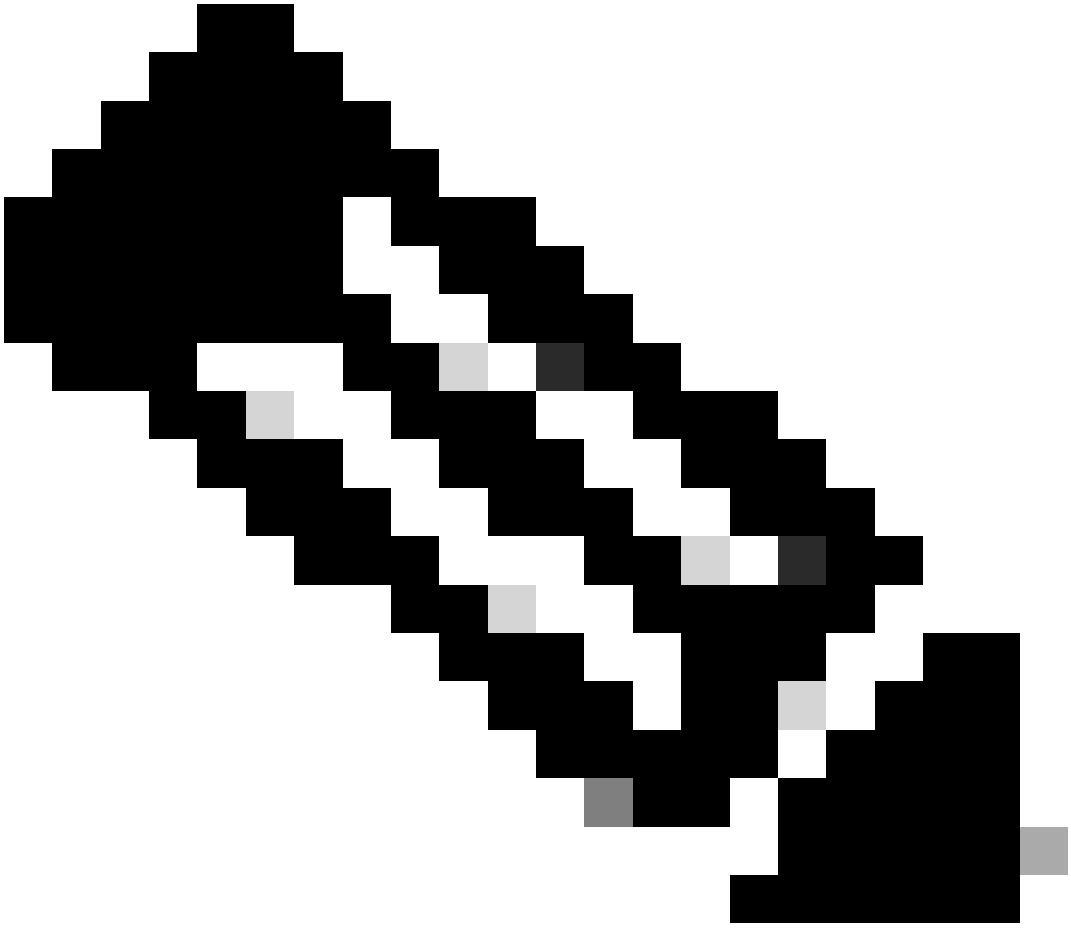
In entrambi gli scenari menzionati in precedenza, si dispone di un'ispezione UTD con una combinazione SS-NAT. Di seguito è riportata la configurazione UTD di esempio per questo scenario.

```
policy utd-policy-vrf-10
 all-interfaces
 vrf 10
 threat-inspection profile TEST_IDS_Policy
 exit
```

Avviso: la combinazione di UTD con SS-NAT non è attualmente supportata. Pertanto, questa combinazione non funziona come previsto. Una soluzione a questo problema potrebbe essere inclusa nelle versioni future.

Soluzione alternativa

Per risolvere il problema, disabilitare il criterio UTD sulla VPN IP sovrapposta (in questo caso la VPN 10) e abilitare la VPN globale.



Nota: questa configurazione è stata testata e verificata nella versione 17.6.

```
policy utd-policy-vrf-global
all-interfaces
vrf global
threat-inspection profile TEST_IDS_Policy
exit
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).